Section IV: Network Security
Title: Remote Access and VPNs Security Standard
Current Effective Date: June 30, 2008
Revision History: May 7, 2008
Original Effective Date: June 30, 2008

Purpose: To secure and protect the network within the North Carolina (NC) Department of Health and Human Services (DHHS) while workforce members are working remotely.

STANDARD

1.0 Background

Authorized users of the DHHS computer systems (e.g., servers, personal computers (PCs), and personal digital assistants (PDAs), etc.), the state's network, and the data repositories shall be permitted to remotely connect to those systems, networks, and data repositories for the sole purpose of conducting DHHS related business. Remote connections shall be accessed only through a secured, authenticated, and protected access method.

Access to the DHHS network shall be permitted as stated in the NC State Office of Information Technology Services (ITS) Security Manual – Statewide Standard for Remote Access. State systems shall only be available for remote authorized access after an explicit request form (i.e., Application and Authorization for Access to State Automated Systems Form or Application and Authorization for Access to DHHS Automated Systems Users, Third-Party, and Vendor Access Form) is submitted by the users and approved by the manager of the system. Each Division and Office shall develop the procedures for remote access.

Opening uncontrolled or unsecured paths into any element of the DHHS network presents *unacceptable* risk to the entire state's network infrastructure.

2.0 DHHS Standard for Remote Access

Remote access to any DHHS resource from an external or a non-state source must originate through a virtual private network (VPN). Any other remote access utilities must have specific authorization from the Division Information Security Official (ISO) for their use.

3.0 Authentication

The Divisions and Offices shall manage the authentication and authorization system for remote access. Those Divisions and Offices that need centralized network infrastructure services, such as public key infrastructure (PKI), shall use the statewide authentication and authorization service, known as the North Carolina Identity Management Service (NCID). The authentication for remote access passwords shall not traverse the network in clear text and must meet minimum password strength requirements, as

documented in approved security policies, procedures, and standards. Each user who remotely accesses an internal network or system shall be uniquely identifiable.

4.0 Users

4.1 User Identifications (IDs)

All users who utilize remote access privileges shall be responsible for the activity performed with their user IDs. User IDs shall not be utilized by anyone but the individuals to whom they have been issued. Users shall be forbidden to perform any activity with user IDs belonging to others. With the exception of Web servers or other systems where all regular users are anonymous, the systems shall not allow anonymously access (e.g., by using guest user IDs).

4.2 Revocation/Modification

Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon a workforce member's termination from service. Remote access privileges shall be reviewed upon a workforce member's change of assignments in conjunction with regularly scheduled security risk assessments.

5.0 Configuration

5.1 Default to Denial

When a computer or network access control system is not functioning properly, it shall default to denial of access privileges to all users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.

5.2 Privilege Access Controls

All computers permanently or intermittently connected to external networks must operate with privilege access controls approved by the DHHS. Multi-user systems must employ user IDs unique to each user, as well as user privilege restriction mechanisms including directories and file access permissions.

5.3 Endpoint Security

External computers or networks that make remote connections to internal state computers or networks must get approval from the Division ISO prior to gaining access. The Division ISO shall ensure that the external devices utilize approved security controls (e.g., antivirus, Firewalls, etc.). The Divisions and Offices shall ensure that updates to virus scanning and other security software are available to users. External computers or networks making a remote connection to a public Web server are exempt.

5.4 Time-Out

Network-connected single user systems shall employ DHHS approved hardware or software mechanisms that control system booting and that include a time-out after inactivity (e.g., screen savers, session time-outs, client-server applications, administrative time-outs, etc.). To the extent possible, all systems accepting remote connections from public network-connected users connected through dial-up phone modems, dial-up Internet service providers, or broadband (i.e., DSL or cable modems) shall include a time-out system. These types of time-out systems must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the DHHS network. In addition, all user IDs registered to networks or computers with external access facilities shall be automatically suspended after a period of thirty (30) days of inactivity.

5.5 Identity Interaction

Creation, deletion, and change of all user IDs performed by System Administrators and others with such privileges shall be securely logged and reviewed on a regular basis.

5.6 Failure to Authenticate

To the extent possible, all systems accepting remote connections from external or non-state systems users shall temporarily terminate the connection or time-out the user ID following three (3) unsuccessful attempts to log-in.

5.7 Modems on Desktop/Laptop Systems

By default, modems on desktop/laptop systems will be disabled. A workforce member supervisor must submit a written request to the Division ISO for approval of the modem and the communication software used with the modem. The Division will keep a record of this approval and the Division ISO will maintain an inventory of enabled modems.

5.8 VPN

All DHHS personal computers, servers, and networking devices must communicate via a VPN and/or other secure protocol when data traverses any open network.

5.9 Client-to-Server

For client-server and/or gateway VPN solutions, split tunneling shall not be permitted via a configuration option.

6.0 Access to Single-Host Systems

6.1 Single-Equipment

Remote access to single-equipment hosts (e.g., DHHS servers, Web hosting equipment, etc.) shall be permitted only if the following criteria are provided to secure and protect DHHS against inherent risk:

- The Divisions and Offices must provide a dial-up modem service that is exclusively limited to their workforce (i.e., employees, contractors, business associates, etc.).
- The Web hosting servers must provide access to pages in order to prevent onward connection to the DHHS Network.

6.2 Management Consoles and Other Special Needs

Users requiring modem access for *Third-Party Provider* management or special needs must obtain the Division ISO's approval for the modem and their use, as set forth in DHHS policies. Each Division and Office shall establish policies and procedures to approve modems on an individual basis. Any dial-up server that grants network access must authenticate each user minimally by a unique identification with a password and shall encrypt the data stream. All calls must be logged and logs of access shall be retained for ninety (90) days for auditing purposes. Modems must not utilize scripts that record the credentials. The dial-up bank should log off inactive users. The period of inactivity for sessions and terminal time-outs shall be established based on the Divisions and Offices needs, systems, the application's criticality, the confidentiality of the information accessed through the systems, applications or other risk factors, but shall not exceed twenty (20) minutes.

7.0 Miscellaneous

7.1 Disclosure of Systems Information

The internal address configurations and related systems design information for the state computers and networks shall be kept confidential. The system information shall not be released to third-party vendors who do not have a demonstrable *need to know* for such information. In addition, the security measures employed to protect the state computers and networks shall be kept protected against any type of inherent risk.

7.2 System Support

Systems shall support the capability to log all remote access occurrences (e.g., user ID, date/time, and duration of connection at a minimum).

7.3 Remote Access Users Transferring Confidential Data

Remote access users who transfer confidential data must utilize end-to-end encryption to protect the data that is sent between the remote access client and the host. For installations where data confidentiality is

always required, remote access servers shall be set to require encrypted communications; users who attempt unencrypted data connections to the server shall have the connection attempt denied.

7.4 Audit

Audit logs of remote access activities shall be maintained for at least ninety (90) days.

Reference:

- NC Statewide Information Technology Security Manual, Version No. 1
  - Chapter 2 – Controlling Access to Information and Systems, Section 01: Controlling Access to Information and Systems
    - Standard 020106 – Managing Passwords
    - Standard 020112 – Controlling Remote User Access
  - Chapter 3 – Processing Information and Documents, Section 01: Networks
    - Standard 030109 – Time-Out Facility
  - Chapter 5 – Securing Software, Peripherals and Other Equipment, Section 02: Cabling, UPS, Printers and Modem
    - Standard 050204 – Using Modems/ISDN/DSL Connections
  - Chapter 5 – Securing Software, Peripherals and Other Equipment, Section 04: Working Off Premises or Using Outsourced Processing
    - Standard 050404 – Working from Home or Other Off-Site Location (Teleworking)
  - Chapter 10 – Addressing Personnel Issues Relating to Security, Section 03: Personnel Information Security Responsibilities
    - Standard 100302 – Keeping Passwords/PIN Numbers Confidential

- NC State Office of Information Technology Security Manual, Statewide Standard for Remote Access
  - Explicit Request Form
    - Application and Authorization for Access to State Automated Systems Form
    - Application and Authorization for Access to DHHS Automated Systems Users, Third-Party, and Vendor Access Form

- NC DHHS Security Standards
  - Administrative Security Standard
    - Personnel Security Standard
  - Network Security Standard
    - Digital Signatures Security Standard
    - Encryption Security Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Network and Telecommunications Security Policy
  - User Authorization, Identification and Authentication Policy